Haut du formulaire

Sélectionnez votre langue  :

Options avancées  :

Mode expert   
Mode debug   
  
Par paquet de 25050010001250150025005000Tout fichiers

Ignorer les fichiers suivant:  :

Archives  
7z, bak, gz, gzip, jpa, tar, zip   
Documents  
doc, docx, pdf, ppt, pptx, xls, xlsx   
Fontes web  
eot, otf, ttf, ttf2, woff, woff2   
Images  
bmp, eps, gif, ico, icon, jpeg, jpg, png, psd, svg, tiff, webp   
Medias (autre qu'images)  
css, js, less   
Animations  
aiff, asf, avi, fla, flv, f4v, m4v, mkv, mov, mp3, mp4, mpeg, mpg, ogg, ogv, swf, wav, webm, wma   
Textes (autre que html)  
ini, json, log, md, mo, po, sql, text, txt, xml, xsl

Appliquer

Bas du formulaire

Joomla 5.1.4 (27-August-2024 16 GMT)

**%s**

[](https://github.com/cavo789/aesecure_quickscan)Ce script va scanner l'ensemble de votre site à la recherche de quelques 'signatures' (patterns) de virus *(pour des raisons de performance, les fichiers de plus de 1M seront ignorés).*L'action du script est de faire un scan : aucune suppression de fichier ne sera faite; il n'y a donc aucun risque de l'exécuter sur votre site.

×Quelques considérations à bien comprendre :

1. Le scan est superficiel et en aucun cas exhaustif; seules quelques signatures sont recherchées alors que les possibilités de hack sont fort nombreuses,
2. si le script détecte la présence de certaines signatures (p.ex. "base64\_decode"), cela n'implique pas que votre site ait été hacké. En effet, certaines instructions sont utilisées lors de hack (base64\_decode) mais sont également utilisées de manière parfaitement légitime dans des codes sources php,
3. Les résultats retournés doivent **TOUJOURS** être correctement compris avant de prendre une quelconque action, demandez de l'aide sur un forum p.ex. si vous doutez.
4. Soyez patient : le scan se fait fichier par fichier et peut donc être plus ou moins long; dépendant de la complexité de votre site.

L'auteur du script décline toute responsabilité en cas de mauvais usage du script ou d'actions prises par le webmaster suite aux résultats mentionnés.

1. Nettoyé 2. 2.081 fichiers 3. Scanner le site  4. Supprimer ce script du serveur

2.081 fichiers vont être analysés (10.905 fichiers ont été ignorés car ils sont repris sur la liste blanche d'aeSecure et 14.718 ignorés comme paramétré dans l'écran des options avancées).

1 -> 500 501 -> 1.000 1.001 -> 1.500 1.501 -> 2.000 2.001 -> 2.081

2081 fichiers ont été analysés dont 35 sont détectés comme potentiellement dangereux.  
0 fichiers ont été ignorés car ayant une taille supérieure ou égale à 1 MB et 0 fichier(s) inaccessible(s) à cause d'un niveau de permission (chmod) trop restreint.

Si les résultats de ce script ont démontré la présence de virus, veuillez bien comprendre que le script a cherché des fichiers connus comme malsain (blacklist) et qu'il a recherché qu'un tout petit nombre de possibilités de hacking. Seules quelques signatures; simples; ont été recherchées. Il faut donc vous attendre à ce que vous ayez d'autres virus sur votre site web et il faudrait considérer un scan complet du site pour les éliminer. N'hésitez pas à me contacter : [https://www.avonture.be](https://www.avonture.be/), je peux nettoyer votre site web.

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\platform\Joomla\Platform.php(29.89K)(Date dernière modif. September 21 2024 09:12:44.)84101925cec16b21f4f04994a6e51104Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **1588** du fichier; voici le contexte :
2. c $dbDriver = null;
3. /\*\*
4. \* Flash variables for the CLI application. We use this array since we're **hell** bent on NOT using Joomla's broken
5. \* session package.
6. \*
7. \* @var array
8. \*

\* @since 5.3.5

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\src\Controller\PushController.php(1.73K)(Date dernière modif. September 21 2024 09:12:44.)efd9c26c2d19ad7aaecb1317bc58a101Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **1515** du fichier; voici le contexte :
2. Name = $this->app->get('sitename');
3. $title = Text::sprintf('COM\_AKEEBABACKUP\_CONTROLPANEL\_WEBPUSH**\_HELL**O\_TITLE', $siteName);
4. $options = new NotificationOptions();

$options->body = Text::\_('COM\_AKEEBA

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **1647** du fichier; voici le contexte :

tions = new NotificationOptions();

$options->body = Text::\_('COM\_AKEEBABACKUP\_CONTROLPANEL\_WEBPUSH**\_HELL**O\_BODY');

$this->getModel()->sendNotification(

$title,

$options->toArray(),

null,

$su

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\src\Helper\Utils.php(3.96K)(Date dernière modif. September 21 2024 09:12:44.)4b5b96cc0c4bb2ae457eea1881394befAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3313** du fichier; voici le contexte :
2. $returnUrl == $encoded) && (strpos($returnUrl, 'index.php') === false))
3. {
4. $possibleReturnUrl = **base64\_decode**($returnUrl);
5. if ($possibleReturnUrl !== false)
6. {
7. $returnUrl = $possibleReturnUrl;

}

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\src\Model\UpgradeHandler\MigrateSettings.php(14.51K)(Date dernière modif. September 21 2024 09:12:44.)1790d0efeb8c1ad9b957bb4d0df59418Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10248** du fichier; voici le contexte :
2. rocess = trim($toProcess, '\'');
3. define('AKEEBA\_MIGRATED\_SERVERKEY', $toProcess);
4. }
5. $key = @**base64\_decode**(AKEEBA\_MIGRATED\_SERVERKEY);
6. if (empty($key))
7. {
8. return;
9. }

$secSettings = Factory::getSe

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\tmpl\commontemplates\errorhandler.php(8.21K)(Date dernière modif. September 21 2024 09:12:44.)2ce85090fd569a36e4bdc4feed9d8526Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5722** du fichier; voici le contexte :
2. T, true)) ?></pre>
3. <h4>$\_POST</h4>
4. <pre><?= htmlentities(print\_r($\_POST, true)) ?></pre>
5. <h4>$**\_COOKIE**</h4>
6. <pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>
7. <h4>$\_REQUEST</h4>

<pre><?= html

Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5768** du fichier; voici le contexte :

= htmlentities(print\_r($\_POST, true)) ?></pre>

<h4>$**\_COOKIE**</h4>

<pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>

<h4>$\_REQUEST</h4>

<pre><?= htmlentities(print\_r($\_REQUEST, true)) ?></pre>

×

1. D: \wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Archiver\BaseArchiver.php(22.35K)(Date dernière modif. September 21 2024 09:12:44.)fffb1b8ece7aa1fc33cc9cf11b6771ceAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **9072** du fichier; voici le contexte :
2. Symlink)
3. {
4. // If we don't have gzip installed we can't compress anything
5. if (!function\_exists("**gzcompress**"))
6. {
7. return 0;
8. }
9. // Don't compress directories or symlinks

if ($isDir || $isSymlink)

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **11874** du fichier; voici le contexte :

$c\_len = $unc\_len;

$compressionMethod = 0;

// Proceed with compression

$zdata = @**gzcompress**($udata);

if ($zdata !== false)

{

// The compression succeeded

unset($udata);

$compres

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Core\Domain\Init.php(14.55K)(Date dernière modif. September 21 2024 09:12:44.)e2ca58f5eb5c0cd738e77bb348c1a91fAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **7409** du fichier; voici le contexte :
2. Factory::getLog()->info("Current mem. usage :" . memory\_get\_usage());
3. }
4. if (function\_exists("**gzcompress**"))
5. {
6. Factory::getLog()->info("GZIP Compression : available (good)");
7. }
8. else

{

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Factory.php(29.06K)(Date dernière modif. September 21 2024 09:12:44.)701ec3fa2d87485779547609ec9192faAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3843** du fichier; voici le contexte :
2. unction unserialize(string $serializedData): void
3. {
4. static::nuke();
5. $engineInfo = unserialize(**base64\_decode**($serializedData));
6. static::$root = $engineInfo['root'] ?? '';

static::$objectLi

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\FixMySQLHostname.php(7.12K)(Date dernière modif. September 21 2024 09:12:44.)2f8cc118542a608d0b68f42d55ad42d3Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6430** du fichier; voici le contexte :
2. be enclosed with parentheses and have \\.\ in front.
3. \*
4. \* @see https://dev.mysql.com/doc/mysql-**shell**/8.0/en/mysql-**shell**-connection-socket.html

\* @see https://www.php.net/manual/en/mysqli.quickstart

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6449** du fichier; voici le contexte :

rentheses and have \\.\ in front.

\*

\* @see https://dev.mysql.com/doc/mysql-**shell**/8.0/en/mysql-**shell**-connection-socket.html

\* @see https://www.php.net/manual/en/mysqli.quickstart.connections.php

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Complexify.php(15.49K)(Date dernière modif. September 21 2024 09:12:44.)cde1af865d468519c69b8bf3c3144037Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **5995** du fichier; voici le contexte :
2. eam',
3. 'david', 'dirty', 'eagle', 'enjoy', 'enter', 'frank', 'girls', 'great', 'green',
4. 'happy', **'hell**o', 'horny', 'house', 'james', 'japan', 'jason', 'juice', 'kelly',

'kevin', 'kitty', 'lover', 'luc

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **chell**Trouvé en position **10110** du fichier; voici le contexte :

otball', 'hardcore',

'iloveyou', 'internet', 'jennifer', 'marlboro', 'maverick', 'mercedes',

'mi**chell**e', 'midnight', 'mistress', 'mountain', 'nicholas', 'password',

'princess', 'qwertyui', 'redskins'

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Encrypt.php(27.24K)(Date dernière modif. September 21 2024 09:12:44.)e5f4f7fd8426505cdb17be7869e79364Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10911** du fichier; voici le contexte :
2. ys
3. if (!($nBits == 128 || $nBits == 192 || $nBits == 256))
4. {
5. return '';
6. }
7. $ciphertext = **base64\_decode**($ciphertext);
8. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nBits / 8

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\FactoryStorage.php(7.11K)(Date dernière modif. September 21 2024 09:12:44.)8ba83d51b1104a0f241ea5eaf9aa94ceAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6428** du fichier; voici le contexte :
2. Index = $isPHPFile ? 2 : 1;
3. switch ($parts[$encodingIndex])
4. {
5. case 'base64';
6. return **base64\_decode**($parts[$dataIndex]);
7. break;
8. case 'uuencode':

return convert\_uudecode($parts[$dataIndex]

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **uudecode**Trouvé en position **6514** du fichier; voici le contexte :

';

return base64\_decode($parts[$dataIndex]);

break;

case 'uuencode':

return convert\_**uudecode**($parts[$dataIndex]);

break;

case 'plain':

return $parts[$dataIndex];

break;

def

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **7007** du fichier; voici le contexte :

ncoding: base sixty four, handled by PHP

if (function\_exists('base64\_encode') && function\_exists('**base64\_decode**'))

{

return 'base64';

}

// Fallback: UUencoding

if (function\_exists('convert\_uuencode')

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **uudecode**Trouvé en position **7149** du fichier; voici le contexte :

}

// Fallback: UUencoding

if (function\_exists('convert\_uuencode') && function\_exists('convert\_**uudecode**'))

{

return 'uuencode';

}

// Final fallback (should NOT be necessary): plain text encodin

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\SecureSettings.php(5.57K)(Date dernière modif. September 21 2024 09:12:44.)91a6d8a1a580a04df26743440489abf7Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2147** du fichier; voici le contexte :
2. include\_once $altFilename;
3. }
4. }
5. if (defined('AKEEBA\_SERVERKEY'))
6. {
7. $this->key = **base64\_decode**(AKEEBA\_SERVERKEY);
8. }
9. }
10. return $this->key;
11. }
12. /\*\*

\* Do the server options allow us to us

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2817** du fichier; voici le contexte :

ncode/\_decode required for encryption?

if (!function\_exists('base64\_encode') || !function\_exists('**base64\_decode**'))

{

return false;

}

// Pre-requisites met. We can encrypt and decrypt!

return true;

}

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5384** du fichier; voici le contexte :

pted = substr($encrypted, 12);

switch ($mode)

{

default:

case 'AES128':

$encrypted = **base64\_decode**($encrypted);

$decrypted = rtrim(Factory::getEncryption()->AESDecryptCBC($encrypted, $key), "\0"

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Transfer\Sftp.php(14.72K)(Date dernière modif. September 21 2024 09:12:44.)078cef39c56c9ce1837de0a003342aebAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **11110** du fichier; voici le contexte :
2. likely to fail) raw command mode
3. else
4. {
5. $cmd = 'chmod ' . decoct($permissions) . ' ' . escape**shell**arg($fileName);
6. return @ssh2\_exec($this->connection, $cmd);
7. }
8. }
9. /\*\*

\* Create a directory

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **14665** du fichier; voici le contexte :

t($folder)

{

// First try the command for Linxu servers

$res = $this->ssh2cmd('ls -l ' . escape**shell**arg($folder));

// If an error occurred let's try the command for Windows servers

if (empty($res

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **14820** du fichier; voici le contexte :

y the command for Windows servers

if (empty($res))

{

$res = $this->ssh2cmd('CMD /C ' . escape**shell**arg($folder));

}

return $res;

}

private function ssh2cmd($command)

{

$stream = ssh2\_exec(

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\webpush\src\Base64Url\Base64Url.php(2.56K)(Date dernière modif. September 21 2024 09:12:44.)4a1453661e97c93fc0b1f18b206192c7Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1658** du fichier; voici le contexte :
2. ===================================================
3. \*/
4. use InvalidArgumentException;
5. use function **base64\_decode**;
6. use function base64\_encode;
7. use function rtrim;
8. use function strtr;
9. /\*\*

\* Encode and decode data

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2454** du fichier; voici le contexte :

alidArgumentException

\*

\*/

public static function decode(string $data): string

{

$decoded = **base64\_decode**(strtr($data, '-\_', '+/'), true);

if (false === $decoded)

{

throw new InvalidArgumentExceptio

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\composer\ca-bundle\res\cacert.pem(223.27K)(Date dernière modif. September 21 2024 09:12:44.)694ccfb21bbe1b997e3e4217d0256ebbAttention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **45420** du fichier; voici le contexte :
2. CzAJBgNVBAYTAlVTMRAw
3. DgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxTdGFyZmllbGQg
4. VG**<="" span="" data-original-title="" title="">">VjaG**5vbG9naWVzLCBJbmMuMTIwMAYDVQQDEylTdGFyZmllbGQgUm9vdCBDZXJ0aWZpY2F0ZSBB

dXRob3JpdHkgLSBHMjCCASIwDQYJK

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **46931** du fichier; voici le contexte :

CzAJBgNV

BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxT

dGFyZmllbGQgVG**<="" span="" data-original-title="" title="">">VjaG**5vbG9naWVzLCBJbmMuMTswOQYDVQQDEzJTdGFyZmllbGQgU2VydmljZXMg

Um9vdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgLSBHM

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **56243** du fichier; voici le contexte :

0Q0EyMB4XDTA5MDUyOTA1MDAzOVoXDTI5MDUyOTA1MDAzOVowXTELMAkGA1UEBhMC

SlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="">">N5c3Rlb**XMgQ08uLExURC4xJzAlBgNVBAsTHlNlY3Vy

aXR5IENvbW11bmljYXRpb24gUm9vdENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEP

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **109420** du fichier; voici le contexte :

gAwIBAgIQIdbQSk8lD8kyN/yqXhKN6TANBgkqhkiG9w0BAQ0FADCBgDELMAkGA1UE

BhMCUEwxIjAgBgNVBAoTGVVuaXpldG8gVG**<="" span="" data-original-title="" title="">">VjaG**5vbG9naWVzIFMuQS4xJzAlBgNVBAsTHkNlcnR1

bSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEkMCIGA1UEAxMbQ2VydHVtIFRyd

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **203762** du fichier; voici le contexte :

0Q0ExMB4XDTE2MDYxNjA1MTUyOFoXDTM4MDExODA1MTUyOFowYTEL

MAkGA1UEBhMCSlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="">">N5c3Rlb**XMgQ08uLExURC4xKzApBgNV

BAMTIlNlY3VyaXR5IENvbW11bmljYXRpb24gRUNDIFJvb3RDQTEwdjAQBgcqhkjOPQIBBgUrgQQA

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **216274** du fichier; voici le contexte :

DQSBHMzAeFw0yMTA1MjAwMjEwMTlaFw00NjA1MTkwMjEw

MTlaMFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="">">VjaG**5vbG9naWVzLCBJbmMu

MSQwIgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzMwggIiMA0GCSqGSIb3DQEBAQUA

A4IC

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **218339** du fichier; voici le contexte :

DQSBHNDAeFw0yMTA1MjAwMjEwMjJaFw00NjA1MTkwMjEwMjJa

MFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="">">VjaG**5vbG9naWVzLCBJbmMuMSQw

IgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzQwdjAQBgcqhkjOPQIBBgUrgQQAIgNi

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_icagenda\src\Utilities\Manager\Manager.php(7.97K)(Date dernière modif. August 28 2024 17:48:12.)7fb4419486f536b0ad4ad5f0615f9e14Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **6684** du fichier; voici le contexte :
2. ias ?: $item->username;
3. $approvedbodycontent = Text::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $creator) . ',<br /><br />';

$approvedbodycontent.= Text::sprintf('COM\_ICAGENDA\_APPROVED\_USER

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_icagenda\utilities\manager\manager.php(6.70K)(Date dernière modif. August 28 2024 17:48:12.)5145b3754e8007c0bc46f24525c5f3a0Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **5793** du fichier; voici le contexte :
2. as ?: $item->username;
3. $approvedbodycontent = JText::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $creator) . ',<br /><br />';

$approvedbodycontent.= JText::sprintf('COM\_ICAGENDA\_APPROVED\_USE

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_jce\helpers\encrypt\aes.php(22.04K)(Date dernière modif. August 31 2024 15:58:02.)0fe3e6c4edd58f48c03dea8497a86012Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14018** du fichier; voici le contexte :
2. = 256)) {
3. return '';
4. } // standard allows 128/192/256 bit keys
5. $ciphertext = **base64\_decode**($ciphertext);
6. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nB

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_jce\helpers\encrypt.php(4.13K)(Date dernière modif. August 31 2024 15:58:02.)7181bf8e9c3b05560e8b832769629075Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1454** du fichier; voici le contexte :
2. ERVERKEY')) {
3. // return key as string
4. if ($legacy) {
5. $key = **base64\_decode**(WF\_SERVERKEY);
6. return $key;
7. }
8. try {

$keyAs

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3205** du fichier; voici le contexte :

switch ($mode) {

case '###AES128###':

$encrypted = **base64\_decode**($encrypted);

$decrypted = @WFUtilEncrypt::AESDecryptCBC($encrypted, $key, 128);

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3891** du fichier; voici le contexte :

encrypted = substr($encrypted, 12);

// base64decode

$decoded = **base64\_decode**($encrypted);

try {

$decrypted = Crypto::decrypt($decoded, $key);

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_phocagallery\controllers\phocagalleryt.php(6.09K)(Date dernière modif. July 18 2024 18:51:34.)21c61385c1fb194c7cb162fa6145f66dAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1247** du fichier; voici le contexte :
2. jexit(Text::\_('JINVALID\_TOKEN'));
3. $fileid = $this->input->get('fileid');
4. $fileid = urldecode(**base64\_decode**($fileid));
5. $model = $this->getModel();
6. echo $model->getFileContent($fileid);

Factory::getApp

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_phocagallery\libraries\phocagallery\file\fileupload.php(30.77K)(Date dernière modif. July 18 2024 18:51:34.)27292920da0888054200d0bf0da951d3Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15191** du fichier; voici le contexte :
2. /\*if ($return) {
3. $app->enqueueMessage( $errUploadMsg, 'error');
4. $app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);
5. exit;
6. } else {

$app->enqueueMessage( $errUploadMs

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15527** du fichier; voici le contexte :

$app->enqueueMessage( $errUploadMsg, 'error');

if ($frontEnd > 0) {

$app->redirect(**base64\_decode**($return));

} else {

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15589** du fichier; voici le contexte :

ontEnd > 0) {

$app->redirect(**base64\_decode**($return));

} else {

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

}

exit;

} else {

$app->enqueueMessage( $err

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15950** du fichier; voici le contexte :

pp->enqueueMessage( Text::\_('COM\_PHOCAGALLERY\_FILE\_ALREADY\_EXISTS'), 'error');

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage(Text::\_('COM\_

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **16377** du fichier; voici le contexte :

eueMessage( Text::\_('COM\_PHOCAGALLERY\_ERROR\_UNABLE\_TO\_UPLOAD\_FILE'), 'error');

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage( Text::\_('COM

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **16803** du fichier; voici le contexte :

$app->enqueueMessage( Text::\_('COM\_PHOCAGALLERY\_SUCCESS\_FILE\_UPLOAD'));

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage( Text::\_('COM

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17169** du fichier; voici le contexte :

R\_UNABLE\_TO\_UPLOAD\_FILE');

if ($return) {

$app->enqueueMessage( $msg);

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

switch ($viewBack) {

case 'phoc

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_icagenda\models\submit.php(40.74K)(Date dernière modif. August 28 2024 17:48:10.)de2910065b023642da9a7cdb15c3d8dcAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **31078** du fichier; voici le contexte :
2. f User Notification Email
3. $adminbodycontent = JText::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $username) . ',<br /><br />';
4. if ($type == 'approval')
5. {

$adminbodycontent.= JText::\_

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **34599** du fichier; voici le contexte :

;

// Set Body of Notification Email

$user\_submit\_body = JText::sprintf('COM\_ICAGENDA\_USER\_EMAIL**\_HELL**O', $username) . ',<br /><br />';

$user\_submit\_body.= JText::sprintf('COM\_ICAGENDA\_EVENT\_SUBMISSIO

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_icagenda\src\Model\SubmitModel.php(41.78K)(Date dernière modif. August 28 2024 17:48:10.)209ec431da8303e7f1b123687cde458dAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **31148** du fichier; voici le contexte :
2. of User Notification Email
3. $adminbodycontent = Text::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $username) . ',<br /><br />';
4. if ($type == 'approval') {

$adminbodycontent.= Text::\_('CO

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **35128** du fichier; voici le contexte :

);

// Set Body of Notification Email

$user\_submit\_body = Text::sprintf('COM\_ICAGENDA\_USER\_EMAIL**\_HELL**O', $username) . ',<br /><br />';

$user\_submit\_body.= Text::sprintf('COM\_ICAGENDA\_EVENT\_SUBMISSION

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\editor.php(45.22K)(Date dernière modif. August 31 2024 15:58:02.)4d9552ff967310e74f9f11586fba09feDanger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12344** du fichier; voici le contexte :
2. lode(',', $stylesheets);
3. // use cookies to store state
4. $settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);
5. // Set active tab

$set

Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12389** du fichier; voici le contexte :

cookies to store state

$settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);

// Set active tab

$settings['active\_tab'] = 'wf-editor-' . $wf->get

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\encrypt.php(22.04K)(Date dernière modif. August 31 2024 15:58:02.)0fe3e6c4edd58f48c03dea8497a86012Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14018** du fichier; voici le contexte :
2. = 256)) {
3. return '';
4. } // standard allows 128/192/256 bit keys
5. $ciphertext = **base64\_decode**($ciphertext);
6. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nB

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\manager\base.php(8.81K)(Date dernière modif. August 31 2024 15:58:02.)937df2eeda429d16c920b6600fd052e4Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8718** du fichier; voici le contexte :
2. filebrowser\_position', $this->getParam('editor.browser\_position', 'bottom')),
3. 'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('ed

Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8758** du fichier; voici le contexte :

editor.browser\_position', 'bottom')),

'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('editor.filebrowser\_search\_depth', 3),

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\vendor\cssmin\src\Colors.php(5.36K)(Date dernière modif. August 31 2024 15:58:02.)9504199f1ce1ba7d7d7dfba451246fa7Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5078** du fichier; voici le contexte :
2. b4513',
3. 'sandybrown' => '#f4a460',
4. 'seagreen' => '#2e8b57',
5. 'sea**shell**' => '#fff5ee',
6. 'slateblue' => '#6a5acd',

'slategray' => '#708090',

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\plugins\spellchecker\config.php(1.81K)(Date dernière modif. August 31 2024 15:58:02.)b56012fca4671635c713eaae185c1743Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **826** du fichier; voici le contexte :
2. $engine = 'browser';
3. break;
4. case 'pspell':
5. case 'pspell**shell**':

$languages = (array) $wf->getParam('spellchecker.languages', 'English=en', '');

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **970** du fichier; voici le contexte :

$wf->getParam('spellchecker.languages', 'English=en', '');

if ($engine === 'pspell**shell**') {

$engine = 'pspell';

}

if (!function\_exists

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\plugins\spellchecker\spellchecker.php(2.75K)(Date dernière modif. August 31 2024 15:58:02.)02a34ca91ceeb0563ed7616722c9d17dAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1992** du fichier; voici le contexte :
2. hecker.engine', 'browser', 'browser');
3. if (($engine === 'pspell' || $engine === 'pspell**shell**') && function\_exists('pspell\_new')) {
4. $classname = 'PSpell';

$conf

×

1. D:\wamp64\www\randophil56.j5.local\libraries\allediaframework\Framework\Color.php(11.68K)(Date dernière modif. July 02 2024 08:52:14.)1122d7cc7ccad5915d61f8c6a368ea89Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6595** du fichier; voici le contexte :
2. 'sandybrown' => '#F4A460',
3. 'seagreen' => '#2E8B57',
4. 'sea**shell**' => '#FFF5EE',
5. 'sienna' => '#A0522D',

'silver'

×

1. D:\wamp64\www\randophil56.j5.local\libraries\allediaframework\Framework\Joomla\Controller\TraitController.php(3.63K)(Date dernière modif. July 02 2024 08:52:14.)4e0fcf1ca91e877134c13551a08ec1beAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2012** du fichier; voici le contexte :
2. $url = $return ?: $this->app->input->getBase64('return');
3. if ($url) {
4. $url = **base64\_decode**($url);
5. } else {
6. $url = new Uri('index.php');

if ($itemId = $this-

×

1. D:\wamp64\www\randophil56.j5.local\modules\mod\_jm\_kick\_cass\tmpl\default.php(23.73K)(Date dernière modif. March 26 2022 14:53:54.)b390f510efd2f44038bf0c5380a6afabDanger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **510** du fichier; voici le contexte :
2. tInstance();
3. $base=$uri->base();
4. $cc\_textdecoration = $params->get('textdedoration', '0');
5. $cc**\_cookie**notice = $params->get('CookieNotice');
6. $cc\_popup = $params->get('Popup');

$cc\_s

Danger Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **6726** du fichier; voici le contexte :

ho $params->get('ShareNumber')?>

}

});

};

</script>

<?php

}

if ($cc**\_cookie**notice){

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

×

1. D:\wamp64\www\randophil56.j5.local\plugins\system\jsvisit\_counter\countries.csv(4.87K)(Date dernière modif. July 15 2024 18:05:06.)dafe3dbc82284db037bf13be273f009aAttention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **chell**Trouvé en position **3829** du fichier; voici le contexte :
2. Marino,SM,674
3. Sao Tome and Principe,ST,678
4. Saudi Arabia,SA,682
5. Senegal,SN,686
6. Serbia,RS,688
7. Sey**chell**es,SC,690
8. Sierra Leone,SL,694
9. Singapore,SG,702
10. Sint Maarten (Dutch part),SX,534

Slovakia,SK,703

×

1. D:\wamp64\www\randophil56.j5.local\plugins\system\jsvisit\_counter\helper.php(41.72K)(Date dernière modif. July 15 2024 18:05:06.)91f496ab02587be313cac66f24236e65Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **BackDoor**Trouvé en position **24570** du fichier; voici le contexte :
2. 'BBBike',
3. 'BDCbot',
4. 'BDFetch',
5. '**BackDoor**Bot',
6. 'BackStreet',
7. 'BackWeb',

'Backlink-Ceck',

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **HackTeam**Trouvé en position **36320** du fichier; voici le contexte :

'Suzuran',

'Swiftbot',

'Szukacz',

'T0P**HackTeam**',

'T8Abot',

'Teleport',

'TeleportPro',

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **38397** du fichier; voici le contexte :

'WebSauger',

'WebStripper',

'WebSucker',

'WebW**hacker**',

'WebZIP',

'Web Auto',

'Web Collage',

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **38956** du fichier; voici le contexte :

'Website Quester',

'Webster',

'Whack',

'W**hacker**',

'Whatweb',

'Who.is Bot',

'Widow',

100%

[© Avonture Christophe 2013-2024 | *aeSecure QuickScan v.2.0.3*](https://github.com/cavo789/aesecure_quickscan)